UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,558	08/16/2001	Massimiliano Antonio Poletto	12221-009001	4255

26161 7590 11/10/2004

FISH & RICHARDSON PC
225 FRANKLIN ST
BOSTON, MA 02110

EXAMINER	
DINH, MINH	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 11/10/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/931,558	POLETTO ET AL.	
	Examiner	Art Unit	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 August 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *8/16/01; 3/25/02*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-21 have been examined.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 10 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 10 recites the limitations "the hardened network" in line 2 and "the log" in line 3. There is insufficient antecedent basis for these limitations in the claim. The limitation "the hardened network" is interpreted as "the redundant network" (claim 1, line 4); the limitation "the log" is interpreted as "a log".

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-13, 15, 17-19 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mansfield ("Towards Trapping Wily Intruders in the Large") in view of Katz et al (4,575,842).

a. Regarding claims 1-3, 11 and 21, Mansfield discloses a method for a data collector to collect data from sampled network traffic comprising:

sampling network packets and generating statistical information about the network flow (Section 3, Detection of Intrusions from traffic-flow signatures; Section 5, Implementations and Results);

parsing the information in the sampled packets and maintaining the information in a log (Section 3, Detection of Intrusions from traffic-flow signatures); and

communicating the generated statistics over a network to a central control center (Section 5, Implementations and Results; Section 3.1, Traffic-flow signature).

Mansfield does not disclose utilizing a hardened, redundant network. Katz discloses utilizing a hardened, redundant network (col. 3, lines 45-51). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Mansfield method to utilize a hardened, redundant network, as taught by Katz, in order to improve the survivability of a network.

b. Regarding claim 4, Mansfield does not disclose that the network is a telephone network. Katz discloses a telephone network (col. 8, lines 16-25). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Mansfield method such that the network is a telephone network, as taught by Katz. Please refer to motivation recited for using a hardened, redundant network as taught by Katz in claims 3.

c. Regarding claim 5, Mansfield further discloses that the information collected by the data collector includes source information and destination information (Table 1; Section 3, Detection of Intrusions from traffic-flow signatures).

d. Regarding claim 6, Mansfield further discloses that the data collector collects the information but does not log the sampled packets (Section 3.1, Traffic-flow signature).

e. Regarding claim 7, Mansfield further discloses that the data collector analyzes the collected statistics and may, if necessary, compose a message that raises an alarm to the control center (Section 5, Implementations and Results).

f. Regarding claim 8, Mansfield further discloses that the data collector includes a communication process to respond to queries concerning characteristics of traffic on the network (Section 5, Implementations and Results).

g. Regarding claim 9, Mansfield further discloses that the queries originate from the control center and are for information pertaining to statistics collected by the data collector (Section 5, Implementations and Results).

h. Regarding claim 10, Mansfield further discloses that the query can be a request to download via the redundant network, a portion of a log of the collected information (Section 5, Implementations and Results).

i. Regarding claim 12, Mansfield further discloses monitoring packet count, which is a parameter of traffic flow, at two levels of granularity (p. 5, 1st par., "The initial threshold will need ... ball rolling"; Section 3.2, Definition of traffic-flow signature).

j. Regarding claim 13, Mansfield further discloses that monitoring the parameter at multiple levels of granularity is used to trace the source of an attack (Section 5, Implementations and Results).

k. Regarding claim 15, Mansfield further discloses applying multi-level analysis monitor TCP packet ratios, repressor traffic and statistics based Layer 3-7 analysis (Section 3.3, Correlating traffic-flow signatures; Section 4, Map-based distributed Intrusion tracing; Table 1; Section 2, Characteristics of Network Intrusions).

l. Regarding claim 17, Mansfield further discloses monitoring network traffic for ICMP packets with broadcast destination addresses (Section 3.4, Experimental evaluation).

m. Regarding claim 18, Mansfield further discloses monitoring network traffic protocol (TCP) or user datagram protocol (UDP) packets addressed to unused ports (Table 1).

n. Regarding claim 19, Mansfield further discloses monitoring network traffic for transmission control protocol (TCP) ACK packets that do not belong to a known connection (Section 4, Map-based distributed Intrusion tracing).

6. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Mansfield in view of Katz as applied to claim 13 above, and further in view of Zait et al (6,665,684).

Mansfield discloses dividing the traffic flow and using memory spaces to track counts of how many packets a data collector examines for a given parameter (p. 5, 1st

par., "The initial threshold will need ... ball rolling"). The memory spaces meet the limitation of buckets.

Mansfield and Katz do not disclose adjusting the number of buckets as the number of buckets approaches a bucket threshold, by combining several buckets into fewer buckets or dividing a bucket into more buckets. Zait discloses adjusting the number of buckets as the number of buckets approaches a threshold, by dividing a bucket into more buckets (col. 10, lines 25-32). Mansfield and Zait are analogous art because they are from a similar problem solving area, efficient storing and searching for data. It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Mansfield and Katz further to adjust the number of buckets as the number of buckets approaches a threshold, by dividing a bucket into more buckets, as taught by Zait, so that the granularity level matches a degree of parallelism when the degree of parallelism exceeds a threshold.

7. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Mansfield in view of Katz as applied to claim 15 above, and further in view of Roesch ("Snort-Lightweight Intrusion Detection for Networks). Mansfield and Katz do not disclose monitoring network traffic for fragmented IP packets. Roesch discloses monitoring network traffic for fragmented IP packets (p. 230, right col., "Snort currently addresses IP fragmentation ... sent by Snort automatically"). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Mansfield and Katz to monitor network traffic for fragmented IP

packets, as taught by Roesch, so that fragmented packet probes and attacks could be logged and alerts could be generated.

8. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Mansfield in view of Katz as applied to claim 15 above, and further in view of Eichstaedt et al (6,662,230). Mansfield and Katz do not disclose monitoring network traffic generated not by a human user over a persistent HTTP connection. Eichstaedt discloses monitoring network traffic generated not by a human user over a persistent HTTP connection (col. 1, lines 49-63; col. 6, lines 20-33). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Mansfield and Katz to monitor network traffic generated not by a human user over a persistent HTTP connection, as taught by Eichstaedt, in order to prevent overcrawling by robots that make too frequent requests.

9. Claims 1-13 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings ("Cryptography And Network Security: Principles and Practice") in view of Katz et al (4,575,842).

a. Regarding claims 1-3, 11 and 21, Stallings disclose a method for a data collector to collect data from sampled network traffic comprising:

sampling network packets and generating statistical information about the network flow (p. 499, "One or more node ... could be valuable"; figures 15.5 and 15.6);

parsing the information in the sampled packets and maintaining the information in a log (p. 499, "The scheme is designed ... host audit record (HAR)"); and

communicating the generated statistics over a network to a central control center (fig. 15.6).

Stallings does not disclose utilizing a hardened, redundant network. Katz discloses utilizing a hardened, redundant network (col. 3, lines 45-51). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Stallings method to utilize a hardened, redundant network, as taught by Katz, in order to improve the survivability of a network.

b. Regarding claim 4, Stallings does not disclose that the network is a telephone network. Katz discloses a telephone network (col. 8, lines 16-25). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Stallings method such that the network is a telephone network, as taught by Katz. Please refer to motivation recited for using a hardened, redundant network as taught by Katz in claims 3.

c. Regarding claim 5, Stallings further discloses that the information collected by the data collector includes source information and destination information (p. 500, "The LAN monitor agent ... such as *rlogin*").

d. Regarding claim 6, Stallings further discloses that the data collector collects the information but does not log the sampled packets (p. 500, "The LAN monitor agent ... such as *rlogin*").

e. Regarding claim 7, Stallings further discloses that the data collector analyzes the collected statistics and may, if necessary, compose a message that raises an alarm to the control center (p. 500, "When suspicious activity is detected ... from other agents").

f. Regarding claim 8, Stallings further discloses that the data collector includes a communication process to respond to queries concerning characteristics of traffic on the network (p. 500, "When suspicious activity is detected ... from other agents"; fig. 15.6).

g. Regarding claim 9, Stallings further discloses that the queries originate from the control center and are for information pertaining to statistics collected by the data collector (p. 500, "When suspicious activity is detected ... from other agents"; fig. 15.6).

h. Regarding claim 10, Stallings further discloses that the query can be a request to download via the redundant network, a portion of a log of the collected information (p. 499, "One or more nodes ... information could be valuable"; fig. 15.6).

i. Regarding claim 12, Stallings further discloses monitoring a parameter of traffic flow at different levels of granularity (p. 495, "The simplest statistical test ... and resource measures").

j. Regarding claim 13, Stallings further discloses that monitoring the parameter at multiple levels of granularity is used to trace the source of an attack (p. 500, "At the lowest level ... file accessed, and the like").

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Hill et al (6,088,804) discloses a system and method for responding to computer network security attacks.

Gleichauf et al (6,499,107) discloses a system and method for adaptive network security using intelligent packet analysis.

Ohta et al, "Detection, Defense, and Tracking of Internet-Wide Illegal Access in a Distributed Manner".

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon - Fri: 9:00 am - 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh
Examiner
Art Unit 2132

MD
11/04/04

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100